

IN THE UNITED STATES DISTRICT COURT  
FOR THE EASTERN DISTRICT OF VIRGINIA  
Newport News Division

UNITED STATES OF AMERICA	)	
	)	
v.	)	Criminal No. 4:16cr16
	)	
EDWARD JOSEPH MATISH, III	)	

---

**DEFENDANT’S REPLY TO GOVERNMENT’S RESPONSE TO  
THIRD MOTION TO SUPPRESS**

Edward Matish, through counsel and pursuant to Local Rule of Criminal Procedure 47(F)(1), submits this Reply to the Government’s Response to Defendant’s Third Motion to Suppress.

\* \* \*

The government’s Response challenges Mr. Matish’s standing to assert a Fourth Amendment claim, defends the constitutionality of the NIT Warrant, and resists suppression as a remedy. The government’s positions lack merit.

**A. Mr. Matish Has Standing to Challenge the Validity of the Warrant that  
Purported to Authorize the Search of His Home Computer.**

In its Response, the government proposes a novel standing theory under which a person lacks standing to challenge the search of his personal home computer. The government cites precisely *zero* cases in which such a restrictive standing doctrine has been applied.

A defendant has standing to challenge the search if he had a “legitimate expectation of privacy in the invaded place.” *United States v. Castellanos*, 716 F.3d 828, 846 (4th Cir. 2013). Here, the government concedes that the NIT Warrant “authorize[d] a search or seizure of information from [Mr. Matish’s] computer.” (ECF No. 53, 5.) Clearly, Mr. Matish had a reasonable expectation of privacy in his personal home computer. *See United States v.*

*Heckenkamp*, 482 F.3d 1142, 1146 (9th Cir. 2007) (“We hold that he also had a legitimate, objectively reasonable expectation of privacy in his personal computer.”); *United States v. Lifshitz*, 369 F.3d 173, 190 (2d Cir. 2004) (“Individuals generally possess a reasonable expectation of privacy in their home computers.”); *see also United States v. Buckner*, 473 F.3d 551, 554 n.2 (4th Cir.2007); *Trulock v. Freeh*, 275 F.3d 391, 403 (4th Cir. 2001). *Cf. Riley v. California*, 134 S. Ct. 2473, 2495 (2014) (assuming standing to challenge search of cell phone). Accordingly, Mr. Matish has standing to challenge the search of his personal home computer. Here, he does so by demonstrating the invalidity of the warrant that purported to authorize this search. Standing is not an issue.

**B. The Magistrate Judge Lacked Jurisdiction to Issue the NIT Warrant Rendering It Void from Inception.**

The government makes several arguments for the magistrate judge’s authority to issue the NIT Warrant. Those arguments are discussed specifically below. But a key flaw underlying the government’s entire conceptualization is the notion that the validity of the NIT Warrant should be judged “as applied” to Mr. Matish. (*See, e.g.*, ECF No. 53, 4.) This reflects a fundamental misunderstanding of the applicable Fourth Amendment standard. The Fourth Amendment requires that a search be conducted pursuant to a valid warrant. Facts “that emerge after the warrant is issued have no bearing on whether or not a warrant was validly issued.” *Maryland v. Garrison*, 480 U.S. 79, 85 (1987). Thus, the government’s repeated refrain that Mr. Matish and his computer were located in the Eastern District of Virginia—facts that did not emerge until after the warrant was executed—have no bearing on whether the NIT Warrant was validly issued.

The NIT Warrant authorized the FBI to search activating computers *wherever located*. See ex. B, at ¶ 46(a). As the government concedes, “The use of the Tor hidden service by the defendant and other Playpen users made it *impossible for investigators to know in what other districts, if any, the execution of the warrant would take place.*” (ECF No. 53, 15 (emphasis added).) ***So the FBI did not—and could not—know where it was searching until after it searched.*** The warrant purporting to authorize such borderless searches was invalid from inception. Accordingly, *all* searches conducted pursuant to the NIT Warrant—including the search of Mr. Matish’s computer—were presumptively unconstitutional warrantless searches. That Mr. Matish was later discovered to have been within the Eastern District of Virginia is irrelevant to whether the NIT Warrant was valid at the time it issued. For the reasons that follow, it was not.

*a. The Plain Language of the Federal Magistrates Act and Rule 41(b) Did Not Authorize the NIT Warrant*

The government’s arguments based on the language of Federal Magistrates Act and Rule 41(b) do not hold water. In the first instance, the government argues that § 636(a) does not restrict the territory over which a magistrate can exercise power, but rather restricts only where a magistrate judge can physically sit. (ECF No. 53, 9 (arguing that “Section 636(a) limits where a magistrate judge may possess such powers, but not necessarily where those powers can have effects”).) This formalistic reading of the Federal Magistrates Act is inconsistent with both the statute’s plain text and prior judicial interpretations.

In *United States v. Strother*, the D.C. Circuit rejected the reading the government proposes here, noting that Congress “was careful to define, in both statute and rule ... the territorial areas in which the force of [magistrates’] authority could be brought to bear.” 578 F.2d 397, 402 (D.C. Cir. 1978). According to the D.C. Circuit, § 636(a) functions “as an

identification of the area within which a magistrate's warrant can validly take effect, and not as a prohibition upon the magistrate's signing that warrant outside the area so defined.”<sup>1</sup> *Id.* Section 636(a) thus embodies the historic common law “principle that a judicial officer's writ cannot run outside her territorial jurisdiction.” *Id.* at 399. *Accord United States v. Levin*, Crim. No. 15-10271, 2016 WL 2596010, at \*4 (D. Mass. May 5, 2016) (holding that “magistrate judge had no jurisdiction to issue such a warrant under the first paragraph of Section 636(a)” because it purported to “authorize a search of property located outside the district where the issuing magistrate judge sat”); *United States v. Arterbury*, Crim. No. 15-182, ECF No. 47 (N.D. Okla. May 12, 2016) (same); *United States v. Krueger*, 809 F.3d 1109, 1121 (10th Cir. 2015) (Gorsuch, J., concurring) (“[Section] 636(a) imposes independent territorial restrictions on the powers of magistrate judges.”). The government cites zero cases supporting its proposed interpretation of § 636(a).

The government next contends that “three separate provisions” of Rule 41(b) support the issuance of the NIT Warrant. (ECF No. 53, 12.) First, the government argues that Rule 41(b)(4)—which authorizes the use of tracking devices—provided sufficient authority to issue the NIT Warrant regardless of the location of the user or his computer. (ECF No. 53, 12-13.) This is the same argument that the government raised in *Levin*. In that case, the court held that “[t]his analogy does not persuade the Court that the NIT properly may be considered a tracking device, regardless of where the ‘installation’ occurred.” *Levin*, 2016 WL 2596010, at \*6. A

---

<sup>1</sup> Section 636(a) was amended by the Federal Judiciary Emergency Special Sessions Act of 2005, PL 109-63, 119 Stat 1993 (Sept. 9, 2005), but both the old and new versions set territorial restrictions governing the reach of a magistrate's power.

provision governing “tracking devices” does not authorize the search of the contents of a personal computer through government malware.

Second, the government argues that because the NIT (*i.e.*, the government’s malware code) was located in the Eastern District of Virginia at the time the warrant was issued, Rule 41(b)(2) applies. (ECF No. 52, 14.) Except “the actual property to be searched was not the NIT nor the server on which it was located, but rather the users’ computers.” *Levin*, 2016 WL 2596010, at \*6. And the users’ computers were located anywhere in the world. “Therefore, Rule 41(b)(2) is inapposite.” *Id.*

Third, the government argues that Rule 41(b)(1) provides authority because “the NIT warrant was issued by a magistrate judge in the district with the strongest known connection to the search.” (ECF No. 53, 15.) Unfortunately for the government, this ‘strongest known connection’ test appears nowhere in the text of Rule 41(b)(1) or any judicial decisions interpreting it. Rule 41(b)(1) gives magistrate judges “authority to issue a warrant to search for and seize a person or property located within the district.” It is undisputed that the NIT Warrant purported to authorize searches of computers without discriminating on the basis of their location. Rule 41(b)(1) focuses on the place to be searched, not the strength of some amorphous ‘connection’ the investigation has to the district. Thus, Rule 41(b)(1) does not provide authority for the issuance of the NIT Warrant.

*b. The Court Should Decline Government’s Invitation to Adopt a “Flexible” and “Broad” Reading Based on “Spirit” of 41 Rather Than Its Text.*

Perhaps recognizing the lack of textual authority for issuance of the NIT Warrant, the government asks the Court to “read Rule 41 broadly, interpreting it to permit searches ... [that] are not explicitly authorized by the text of the Rule.” (ECF No. 53, 17.) The Court should decline this invitation.

Courts must give the Federal Rules of Procedure “their plain meaning.” *Bus. Guides, Inc. v. Chromatic Commc’ns Enterprises, Inc.*, 498 U.S. 533, 540 (1991). “As with a statute, [the court’s] inquiry is complete if [it] find[s] the text of the Rule to be clear and unambiguous.” *Id.*, see also *Libretti v. United States*, 516 U.S. 29, 51 (1995) (basing decision on “the plain language” of the Rule). Federal Rule of Criminal Procedure 41 “is, in every pertinent respect, as binding as any statute duly enacted by Congress, and federal courts have no more discretion to disregard the Rule’s mandate than they do to disregard constitutional or statutory provisions.” *Bank of Nova Scotia v. United States*, 487 U.S. 250, 255 (1988). For that reason, the Supreme Court has been clear that—whatever the scope of a court’s “inherent power”—“it does not include the power to develop rules that circumvent or conflict with the Federal Rules of Criminal Procedure.” *Carlisle v. United States*, 517 U.S. 416, 426 (1996). Although the government advocates for a “broad,” “flexible” interpretation that focuses on “the spirit of Rule 41,” the proper inquiry is textual, not spiritual. And the NIT Warrant was simply not authorized by Rule 41(b)’s plain text.

### **C. Warrantless Searches of Personal Home Computers Are Unreasonable.**

The government argues that—accepting the FBI’s search as warrantless—the search may still have been “reasonable” and thus allowable under the Fourth Amendment. (ECF No. 53, 18-21.) “In the absence of a warrant, a search is reasonable only if it falls within a specific exception to the warrant requirement.” *Riley*, 134 S. Ct. at 2482. The government relies on the ‘exigent circumstances’ exception. (ECF No. 53, 19.) This exception applies “when the exigencies of the situation make the needs of law enforcement so compelling that a warrantless search is objectively reasonable under the Fourth Amendment.” *Kentucky v. King*, 563 U.S. 452, 460 (2011) (internal quotation marks and brackets omitted).

Circumstances that may give rise to an exigency sufficient to justify a warrantless search include law enforcement's "need to provide emergency assistance to an occupant of a home, engage in 'hot pursuit' of a fleeing suspect, or enter a burning building to put out a fire and investigate its cause." *Missouri v. McNeely*, 133 S. Ct. 1552, 1558-59 (2013) (internal citations omitted). Courts have also applied the exception where a warrantless search is necessary "to prevent the imminent destruction of evidence." *Id.* But in each of these circumstances, the Supreme Court has found that a "warrantless search is potentially reasonable" for the same reason: "there is compelling need for official action *and no time to secure a warrant.*" *Id.* at 1559.

The defense is aware of no case in which the exigent circumstances exception has been applied when the government actually obtained an invalid warrant. The government certainly cites no such example. Indeed, the fact that the government obtained a warrant itself demonstrates that the government had time to secure one. *See Laughter v. Kay*, 986 F. Supp. 1362, 1375 (D. Utah 1997) (finding exigent circumstance argument "frivolous" because "fact that defendants actually obtained a search warrant tends to negate their argument"). By its terms, the exigent circumstances exception applies only when the government had no time to secure a warrant. So it does not apply here.

What the government really wants is a bold new exception to the Fourth Amendment's warrant requirement: When the Executive fails to obtain a valid warrant, it should be able to search people's houses and effects if it has a really good reason.<sup>2</sup> Alas, this is precisely the sort

---

<sup>2</sup> The government's justification for its worldwide warrantless searches is itself questionable. The government argues: "Playpen enabled ongoing sexual abuse and exploitation of children, and deploying the NIT against Playpen users was necessary to stop the abuse and exploitation and to identify and apprehend abusers. Such abuse and exploitation included [ ] the

of roving Executive discretion that the Fourth Amendment's Warrant Clause was designed to prevent. As the Supreme Court recently wrote in *Riley*, "the warrant requirement is 'an important working part of our machinery of government,' not merely 'an inconvenience to be somehow "weighed" against the claims of police efficiency.'" *Riley*, 134 S.Ct. at 2493 (quoting *Coolidge v. New Hampshire*, 403 U.S. 443, 481 (1971)). With the government unable to rely on a specific, established exception to the warrant requirement, the warrantless search here violated the Fourth Amendment.

#### **D. Suppression Is Warranted.**

The government argues that suppression is not an appropriate remedy but provides virtually no legal support for its position.

##### *a. The Good-Faith Exception Does Not Preclude Suppression for the Fourth Amendment Violation.*

The government does not even develop a good faith argument in its Response, including but one conclusory sentence that "the good faith exception bars suppression here." (ECF No. 53, 25.) Insofar as this argument is even properly preserved, it is erroneous.

As an initial matter, courts evaluating this precise NIT Warrant have held that the "good-faith exception" does not apply because the warrant was void from inception. *Levin*, 2016 WL 2596010, at \*10. Other courts, too, have found that the good faith exception does not apply when the warrant itself is void. The Supreme Court of Kentucky wrote,

---

online sexual exploitation of children through the distribution and receipt of child pornography...." (ECF No. 53, 19-20.) But the *government* was operating Playpen. Thus, the government did not need to deploy an NIT or search Mr. Matish's computer to stop the distribution of child pornography on the Playpen site. The government just needed to shut down its own distribution operation. Moreover, the government's own illegal actions—*i.e.*, its distribution of child pornography—created the "exigency" upon which the government relies. *See King*, 563 U.S. at 462.



In *Leon*, the Supreme Court of the United States held that evidence obtained as a result of a search warrant which later was determined to be technically deficient would not be suppressed if the police acted with objective reasonableness in relying on the warrant. However, in the case at bar, we are not confronted with a technical deficiency; but rather a question of jurisdiction. We do not believe that *Leon* would be applicable were we otherwise inclined to follow its precedent.

*Commonwealth v. Shelton*, 766 S.W.2d 628, 629-30 (Ky. 1989).

*Leon*'s good faith exception prevents the automatic suppression of evidence from subsequently invalidated warrants because of the Supreme Court's recognition that "[r]easonable minds frequently may differ on the question whether a particular affidavit establishes probable cause." *United States v. Leon*, 468 U.S. 897, 914 (1984). Thus, the Supreme Court "concluded that the preference for warrants is most appropriately effectuated by according 'great deference' to a magistrate's determination" of probable cause. *Id.* "*Leon* contains not the slightest suggestion, however, that the same deference ought apply when magistrate judges determine their own jurisdiction." *Levin*, 2016 WL 2596010, at \*10. Neither *Leon*'s holding nor its reasoning "contemplate[d] a situation where a warrant is issued by a person lacking the requisite legal authority." *United States v. Scott*, 260 F.3d 512, 515 (6th Cir. 2001) *overruled by United States v. Master*, 614 F.3d 236, 243 (6th Cir. 2010).

Even if *Leon*'s good faith exception was theoretically applicable to warrants void at inception, it should not apply here. As explained in the underlying Motion, the government here knew that NIT remote searches were outside the jurisdiction of a magistrate. Although the affidavit's phrasing is cagey at various points, the government obviously sought a warrant that violated the territorial limits of Rule 41(b). Thus, "it is quite a stretch to label the government's actions in seeking a warrant so clearly in violation of Rule 41 as motivated by 'good faith.'" *United States v. Glover*, 736 F.3d 509, 516 (D.C. Cir. 2013). If suppression is meant to deter

overzealous law enforcement by imposing real consequences for the violation of clear rules, suppression is appropriate here.

*b. Even Assuming No Constitutional Violation, Rule 41 Deficiency Still Requires Suppression.*

The government and defense agree on the applicable standard: Even absent a constitutional violation, suppression is still warranted for a violation of Rule 41 “when a defendant is prejudiced by the violation, or when there is evidence of intentional and deliberate disregard of a provision of the Rule.” (ECF No. 53, 25 (quoting *United States v. Simons*, 206 F.3d 392, 402 (4th Cir. 2000)).)

Prejudice exists when the “the Government would not have obtained [the warrant] had Rule 41(b)(1) been followed.” *United States v. Krueger*, 809 F.3d 1109, 1116 (10th Cir. 2015). Here, the magistrate ***could not*** have issued an NIT Warrant that followed Rule 41. The whole point of the NIT Warrant was to search computers ***to determine their location***. Before deploying the NIT, the government did not know where it was searching. Thus, the only way to follow Rule 41 was not to issue an NIT warrant at all. Mr. Matish was prejudiced.

Moreover, ample evidence points to an intentional and deliberate disregard of Rule 41(b). The government stated in its warrant application that it was seeking authority to search activating computers “wherever located.” Ex. B, at ¶ 46. Still, the cover sheet of its warrant application states that the government requested only authority to search “property ... located in the Eastern District of Virginia.” Ex. B, at 1. While making these seemingly contradictory sworn statements in an attempt to obtain the NIT Warrant, the government was aware of judicial decisions holding that an NIT could not be authorized under Rule 41(b) and the DOJ was lobbying the Rules Committee for a rule change to Rule 41(b) that would authorize such searches. When the

government decided to go ahead with the NIT in this case, it did so intentionally and with deliberate disregard for the territorial restrictions imposed by Rule 41(b). Accordingly, suppression is warranted.

\* \* \*

The NIT Warrant purported to authorize thousands of searches of personal home computers located around the world. What is more, the technology made it impossible for the government to know where it was searching until after its search was complete. A federal magistrate judge cannot authorize blind, worldwide searches of people's electronic effects. So "the NIT Warrant was issued without jurisdiction and thus was void *ab initio*." *Levin*, 2016 WL 2596010, at \*15. "Since warrantless searches are presumptively unreasonable, and the good-faith exception is inapplicable, the evidence must be excluded." *Id.*

Respectfully submitted,

EDWARD JOSEPH MATISH, III

By: \_\_\_\_\_/s/\_\_\_\_\_

Andrew W. Grindrod  
VSB # 83943  
Assistant Federal Public Defender  
Attorney for Edward Joseph Matish, III  
Office of the Federal Public Defender  
150 Boush Street, Suite 403  
Norfolk, Virginia 23510  
(757) 457-0800  
(757) 457-0880 (telefax)  
andrew\_grindrod@fd.org

Richard J. Colgan  
VSB # 19635  
Attorney for Edward Joseph Matish, III  
Office of the Federal Public Defender  
150 Boush Street, Suite 403  
Norfolk, Virginia 23510  
(757) 457-0808

(757) 457-0880 (telefax)  
richard\_colgan@fd.org

**CERTIFICATE OF SERVICE**

I certify that on the 17th day of May, 2016, I will electronically file the foregoing with the Clerk of Court using the CM/ECF system, which will send a notification of such filing (NEF) to the following:

Kaitlin Courtney Gratton, Esq.  
Eric Hurt, Esq.  
United States Attorney's Office (Newport News)  
721 Lakefront Commons  
Suite 300  
Newport News, VA 23606  
(757) 591-4000

By: \_\_\_\_\_/s/\_\_\_\_\_

Andrew W. Grindrod  
VSB # 83943  
Assistant Federal Public Defender  
Attorney for Edward Joseph Matish, III  
Office of the Federal Public Defender  
150 Boush Street, Suite 403  
Norfolk, Virginia 23510  
(757) 457-0800  
(757) 457-0880 (telefax)  
andrew\_grindrod@fd.org